

2661

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the application of:

H. Joiner et al.

Application No. 10/029,591

Filed: 12/21/2001

For: SYSTEM, METHOD AND COMPUTER  
PROGRAM PRODUCT FOR A NETWORK  
ANALYZER BUSINESS MODEL

Group Art Unit: 2661

Examiner: Unassigned

Atty. Docket No. NAI1P063/  
01.305.01

Date: July 22, 2004

RECEIVED

JUL 30 2004

Technology Center 2600

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail in an envelope addressed to: Commissioner for Patents, Alexandria, VA 2213-1450 on July 22, 2004.

Signed:

Erica L. Farlow

INFORMATION DISCLOSURE STATEMENT  
UNDER 37 CFR §§1.56 AND 1.97(b)

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

RECEIVED

AUG 09 2003

GROUP 3600

Dear Sir:

The references listed in the attached PTO Form 1449(s), [at least one of which was provided by an Examiner(s) handling a related patent application(s)], copies of which are attached, may be material to examination of the above-identified patent application. Applicants submit these references in compliance with their duty of disclosure pursuant to 37 CFR §§ 1.56 and 1.97. The Examiner is requested to make these references of official record in this application.



COPY

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/029,686	12/21/2001	Herbert V. Joiner	NA11P065/01.307.01	3317
28875	7590	07/02/2004	EXAMINER	
SILICON VALLEY INTELLECTUAL PROPERTY GROUP P.O. BOX 721120 SAN JOSE, CA 95172-1120			SON, LINH L D	
			ART UNIT	PAPER NUMBER
			2135	8
DATE MAILED: 07/02/2004				

Please find below and/or attached an Office communication concerning this application or proceeding.

RECEIVED  
JUL 30 2004  
Technology Center 2600

RECEIVED  
AUG 09 2003  
GROUP 3600

**Office Action Summary****Application No.**

10/029,686

**Applicant(s)**

JOINER, HERBERT V.

**Examiner**

Linh LD Son

**Art Unit**

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 21 December 2001.  
2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.  
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-24 is/are pending in the application.  
4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.  
5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.  
6) ☒ Claim(s) 1-24 is/are rejected.  
7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.  
8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

RECEIVED  
JUL 30 2004  
Technology Center 2600

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.  
10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).  
11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
a) ☐ All b) ☐ Some \* c) ☐ None of:  
1. ☐ Certified copies of the priority documents have been received.  
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

RECEIVED  
AUG 09 2003  
GROUP 3600

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892)  
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)  
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date 2-3  
4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_  
5) ☐ Notice of Informal Patent Application (PTO-152)  
6) ☐ Other: \_\_\_\_\_

## DETAILED ACTION

### *Information Disclosure Statement*

For IDS (paper #2), the IDS fails to comply with 37 CFR 1.98 (a)(11), which requires a list of all patents, publications, or other info submitted for consideration by the Office. It has been placed in the application file, but the info therein has not been considered.

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.
2. Claims 1, 3-6, 8-11, 13-16, and 18-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Drake et al, hereinafter "Drake", (US/6347374A1).
3. As per claims 1, 3, 6, 8, 11, 13, 16, 18, and 21, Drake discloses the "Event Detection" invention, which includes a method for analyzing a network, scanning the network, and detecting intrusions in the network. The system comprises: Collector (agent), Parsers, Generic File Transfer Utility (GFTU), Inserter, Database, Expert System Engines (ESG) (Host Controller), and Manager/configuration GUI (Zone Controller) (See Fig 1). The collector is an agent running on computers on the network and there are different collectors associated to the applications monitoring (Col 9 lines 53-59). GFTU, located on the client computer, sends data files, such as log files or other files depending on

the application to the Parser (Col 9 line 65 to Col 10 line 4). The Parser is located on the remote network collecting the data files, parses, and then passes the data files in Virtual Record format readable by the ESG to the Inserter (Col 7 lines 38-54, and Col 10 lines 21-32). The Inserter stores the records in the database. The ESG has many functions or controllers, such as deriving database information to detect events, Hard-Coded processor, Execution array-based processors, and Rule-based interpreters (Col 11 lines 7-17, line 52 to Col 13 line 67). ESG utilizes the controllers above to analyze and detect intrusion (Col 7 line 51, and Col 11 line 53 Col 12 line 67), and creates events model and report for the network (Col 15 lines 59-62). The Manager/configuration GUI takes all the output data from ESG and generates reports or statistical data accordingly (Col 17 lines 1-24). The Manager/Configuration GUI also has admin capability to configure rule-based triggers to the event. However, Drake does not teach the Zone Controller specifically. Nevertheless, Drake teaches the ESG, which has the HC and ZC functionalities as claimed and part is in the Manager/Configuration GUI (See above citing). Therefore, it is obvious at the time of the invention for one of ordinary skill in the art to separate both components to minimize the processing time and load.

4. As per claims 4, 9, 14, and 19, Drake discloses the system as recited in claim 1, wherein the host controllers and the zone controllers operate based on business rules (Col 17 lines 15-24).

5. As per claims 5, 10, 15, and 20, Drake and disclose the system as recited in claim 1, wherein the business rules are user-configurable (Col 17 lines 15-24).
6. As per claim 22, claim 1 rejection basis is applied. Further, Drake discloses a method to configure and identifying the business rules applicable to the network users and services (Col 5 lines 36-60 and Col 17 lines 1-24).
7. Claims 2, 7, 12, 17, 23, and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Drake et al, hereinafter "Drake", (US/6347374A1) in view of Eschelbeck (US/6553378B1).
8. As per claims 2, 7, 12, and 17, Drake discloses the system as recited in claim 1. However, Drake does not teach the host controllers are further capable of cyber cop services. Nevertheless, Eschelbeck discloses the "System and process for reporting network events with a plurality of hierarchically-structured databases in a distributed computing environment" invention, which teaches a method of analyzing, detecting, and response to a network node anomaly, such as intrusion, virus attack, and network attack (See Fig. 2). The system includes agents, event detectors and analyzer, and root snap-in agent. The event responding includes forwarding a snap-in component to control the anomaly (Col 7 lines 52-63 and Col 10 line 34 to Col 12 line 8). One of the snap-in

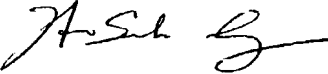
components is the cyber cop service (Eschelbeck, Col 5 line 34). Therefore, it is obvious at the time of the invention was made for one of ordinary skill in the art to incorporate the teaching to resolve the problem in the network.

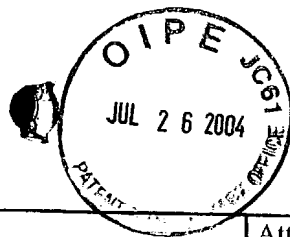
9. As per claims 23 and 24, Claim 1 rejection is incorporated. However, Drake does not teach the anti-virus services. Nevertheless, Eschelbeck teaches the implementation of the anti-virus services (Col 7 lines 1-13). Therefore, it is obvious at the time of the invention for one of ordinary skill in the art to incorporate the service to check the data integrity in the network.

### Conclusion

1. Any inquiry concerning this communication from the examiner should be directed to Linh Son whose telephone number is (703)-305-8914 or Fax to 703-746-9821.
2. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor Kim Y. Vu can be reached at (703)-305-4393. The fax numbers for this group are (703)-872-9306 (official fax). Any inquiry of general nature or relating to the status of this application or proceeding should be directed to the group receptionist whose telephone number is (703)-305-9600.

Linh LD Son  
Patent Examiner

  
AU 2135

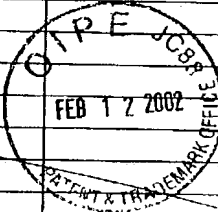


#3

<b>Form 1449 (Modified)</b>  <b>Information Disclosure Statement By Applicant</b>  (Use Several Sheets if Necessary)	Atty. Docket No. NA11P065/01.307.01	Application No.: 10/029,686
	Applicant: H. Joiner	
	Filing Date: 12/21/2001	Group Art Unit: Unassigned

**U.S. Patent Documents**

Examiner Initial	No.	Patent No.	Date	Patentee	Class	Sub-class	Filing Date
H3	A	6,314,460	11/06/2001	Knight et al.	709	220	10/30/1998
HS	B	6,266,694	07/24/2001	Duguay et al.	709	223	06/19/1997
	C						
	D						
	E						
	F						
	G						
	H						
	I						
	J						
	K						



**RECEIVED**  
FEB 15 2002  
Technology Center 2100

**Foreign Patent or Published Foreign Patent Application**

Examiner Initial	No.	Document No.	Publication Date	Country or Patent Office	Class	Sub-class	Translation	
							Yes	No
H3	L	01/84270	11/08/2001	WIPO	G06F	--		
HS	M	01/55862	08/02/2001	WIPO	G06F	13/00		
HS	N	01/31539	05/03/2001	WIPO	G06F	17/60		
HS	O	00/77687	12/21/2000	WIPO	G06F	17/30		
HS	P	00/08806	02/17/2000	WIPO	H04L	12/26		
HS	Q	98/42103	09/24/1998	WIPO	H04L	12/26		

**Other Documents**

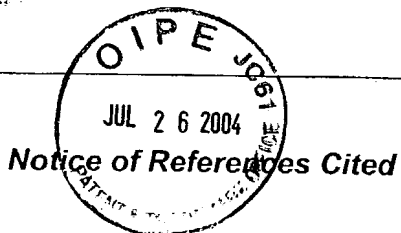
Examiner Initial	No.	Author, Title, Date, Place (e.g. Journal) of Publication
	R	
	S	
	T	
Examiner	Date Considered	

**RECEIVED**  
JUL 30 2004  
Technology Center 2600

Examiner: Initial citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

**RECEIVED**  
AUG 09 2003  
GROUP 3600





Application/Control No. <del>10/029,686</del> 10/029,591	Applicant(s)/Patent Under Reexamination JOINER, HERBERT V.	
	Examiner Linda D. Son Unassigned	Art Unit 2135

Page 1 of 1

### U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
	A	US-6,347,374 B1	02-2002	Drake et al.	713/200
	B	US-6,553,378 B1	04-2003	Eschelbeck, Gerhard	707/10
	C	US-2002/0087882 A1	07-2002	Schneier et al.	713/201
	D	US-2003/0051026 A1	03-2003	Carter et al.	709/224
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

RECEIVED  
 AUG 09 2003  
 GROUP 3600

### FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

### NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

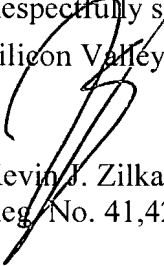
RECEIVED  
 JUL 30 2004  
 Technology Center 2600

\*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)  
 Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

This Information Disclosure Statement is not to be construed as a representation that a search has been made, that additional information material to the examination of this application does not exist, or that these references indeed constitute prior art.

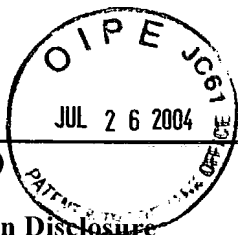
This Information Disclosure Statement is believed to be filed before the mailing date of a first Office Action on the merits. Accordingly, it is believed that no fees are due in connection with the filing of this Information Disclosure Statement. However, if it is determined that any fees are due, the Commissioner is hereby authorized to charge such fees to Deposit Account 50-1351 (Order No. NA11P063).

Respectfully submitted,  
Silicon Valley IP Group, PC



Kevin J. Zilka  
Reg. No. 41,429

P.O. Box 721120  
San Jose, CA 95172-1120  
Telephone: (408) 971-2573



RECEIVED

JUL 3 0 2004

Technology Center 2600

<b>Form 1449 (Modified)</b>  <b>Information Disclosure Statement By Applicant</b>  (Use Several Sheets if Necessary)	Atty. Docket No. NAIIP063/01.305.01	Application No. 10/029,591
	Applicant: H. Joiner et al. Filing Date: 12/21/2001	Group Art Unit: 2661

**U.S. Patent Documents**

Examiner Initial	No.	Patent No.	Date	Patentee	Class	Sub-class	Filing Date
	A						
	B						
	C						
	D						
	E						

**Foreign Patent or Published Foreign Patent Application**

Examiner Initial	No.	Document No.	Publication Date	Country or Patent Office	Class	Sub-class	Translation	
							Yes	No
	F							
	G							
	H							
	I							
	J							
	K							

**Other Documents**

Examiner Initial	No.	Author, Title, Date, Place (e.g. Journal) of Publication
	L	USPTO Office Action mailed 07/02/2004 in application no. 10/029,686, filed 12/21/2001.
	M	
	N	
	O	
	P	
	Q	
	R	
Examiner		Date Considered

Examiner: Initial citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

AUG 0 9 2003

GROUP 3600